In the claims:

All claims presented for examination are listed below.

1. (Currently amended) An apparatus to provide security for ~~secure~~ online transactions ~~on the Internet~~ comprising:

~~a card reader plugged into a microphone input of the PC sound card;~~

a smart card ~~inserted in the card reader for~~ transmitting an identification sequence, as a modulated voltage signal in a frequency range and voltage amplitude compatible with a microphone input of a personal computer (PC) sound card ~~to the microphone input of the PC~~ ~~in the form of a modulated signal~~;

[[and]]

a connector connecting an output of the smart card transmission to the microphone input of the PC sound card; and

a PC applet, executed by the PC, demodulating the identification sequence[[;]]

~~characterized by the absence of processing means within the card reader~~.

2. (Previously presented) The apparatus of claim 1, wherein the identification sequence comprises at least a unique card number and a random number valid only once.

3. (Previously presented) The apparatus of claim 2, wherein the random number is a session key (Ki) which is not transmitted to the authentication server.

4. (Previously presented) The apparatus of claim 3, wherein the session key (Ki) is a function of the previous one (Ki-l) emitted by the card, wherein Ki G(Ki-1) and G is a one-way function also known by the authentication server.

5. (Previously presented) The apparatus of claim 4, wherein the session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password

entered by the user; said first MAC is transmitted to the authentication server along with the card number.

6. (Previously presented) The apparatus of claim 5, wherein the authentication server generates a second MAC of the password stored in the authentication server database, using a session key deduced from the previous one (Ki-1) also stored in the database.

7. (Previously presented) The apparatus of claim 6, wherein the authentication is valid only if said first and second MAC are identical; if this is the case, the authentication server replaces (Ki- 1) by (Ki) in the database and (Ki) cannot be reused.

8. (Previously presented) The apparatus as in claim 1, wherein the smart card is powered by the voltage provided by the microphone input of the PC sound card.

9. (Currently amended) The apparatus as in claim 8, wherein the smart card transmits the modulated signal when [[the]] a switch of the ~~card reader~~ connector is pressed by the user.

10. (Currently amended) The apparatus as in claim 9, wherein the smart card transmits the modulated signal to the microphone input through [[the]] an ISO contact C6.

11. (Currently amended) The apparatus as in claim 10, wherein the smart card transmits the modulated signal when [[the]] an ISO contact C2 is pulled down.

12. (Currently amended) The apparatus as in claim 11, wherein the smart card is powered through [[the]] ISO contacts C4 and C8.

13. (Currently amended) The apparatus as in claim 1, wherein the ~~card reader~~ connector further comprises a battery cell powering the smart card; said ~~reader~~ connector is alternatively plugged into the line input of the PC sound card.

14. (Canceled)

15. (Currently amended) The apparatus as in claim 1, wherein the ~~card reader~~ connector is further integrated into the PC unit or display.

16. (Currently amended) A method for ~~securing online~~ providing security for online transactions ~~on the Internet~~ comprising:

(a) ~~providing~~ inserting a smart card ~~inserted~~ in a ~~card reader~~ connector for connecting an output of the smart card transmission to a microphone input of a PC sound card, in a PC;

(b) transmitting an identification sequence, as a modulated voltage signal in a frequency range and voltage amplitude compatible with a microphone input of a PC sound card, from the smart card directly to [[a]] the microphone input of the PC sound card ~~in the form of a modulated signal~~;

~~(b) plugging the card reader into the microphone input of the PC sound card the card reader devoid of processing means;~~

~~(c) transmitting the modulated signal directly from the smart card to the microphone input of the PC via the card reader;~~ and

(d) demodulating the identification sequence by a PC applet, executed by the PC.

17. (Currently amended) The method of claim [[1]] 16, wherein the identification sequence in step (a) comprises at least a unique card number and a random number valid only once.

18. (Previously presented) The method of claim 17, wherein the random number is a session key (Ki) which is not transmitted to the authentication server.

19. (Currently amended) The method of claim 18, wherein the session key (Ki) is a function of the previous one (Ki-l) emitted by the smart card, wherein Ki G(Ki-1) and G is a one-way function also known by the authentication server.

20. (Currently amended) The method of claim 18, wherein the session key (Ki) is used by the PC applet to generate a message authentication code (MAC) of the password entered by the user; said first MAC is transmitted to the authentication server along with the smart card number.

21. (Previously presented) The method of claim 20, wherein the authentication server generates a second MAC of the password stored in the authentication server database, using a session key deduced from the previous one (Ki-1) also stored in the database.

22. (Previously presented) The method of claim 21, wherein the authentication is valid only if said first and second MAC are identical; if this is the case, the authentication server replaces (Ki- 1) by (Ki) in the database and (Ki) cannot be reused.